FTF 2016
TECHNOLOGY FORUM

MIFARE PLUS PRODUCT FAMILY

BRINGING BENCHMARK AES SECURITY TO CONTACTLESS SMART CARD APPLICATIONS

MARTIN LIEBL
DIRECTOR PRODUCT MANAGEMENT
FTF-CIT-N1926
MAY 17, 2016

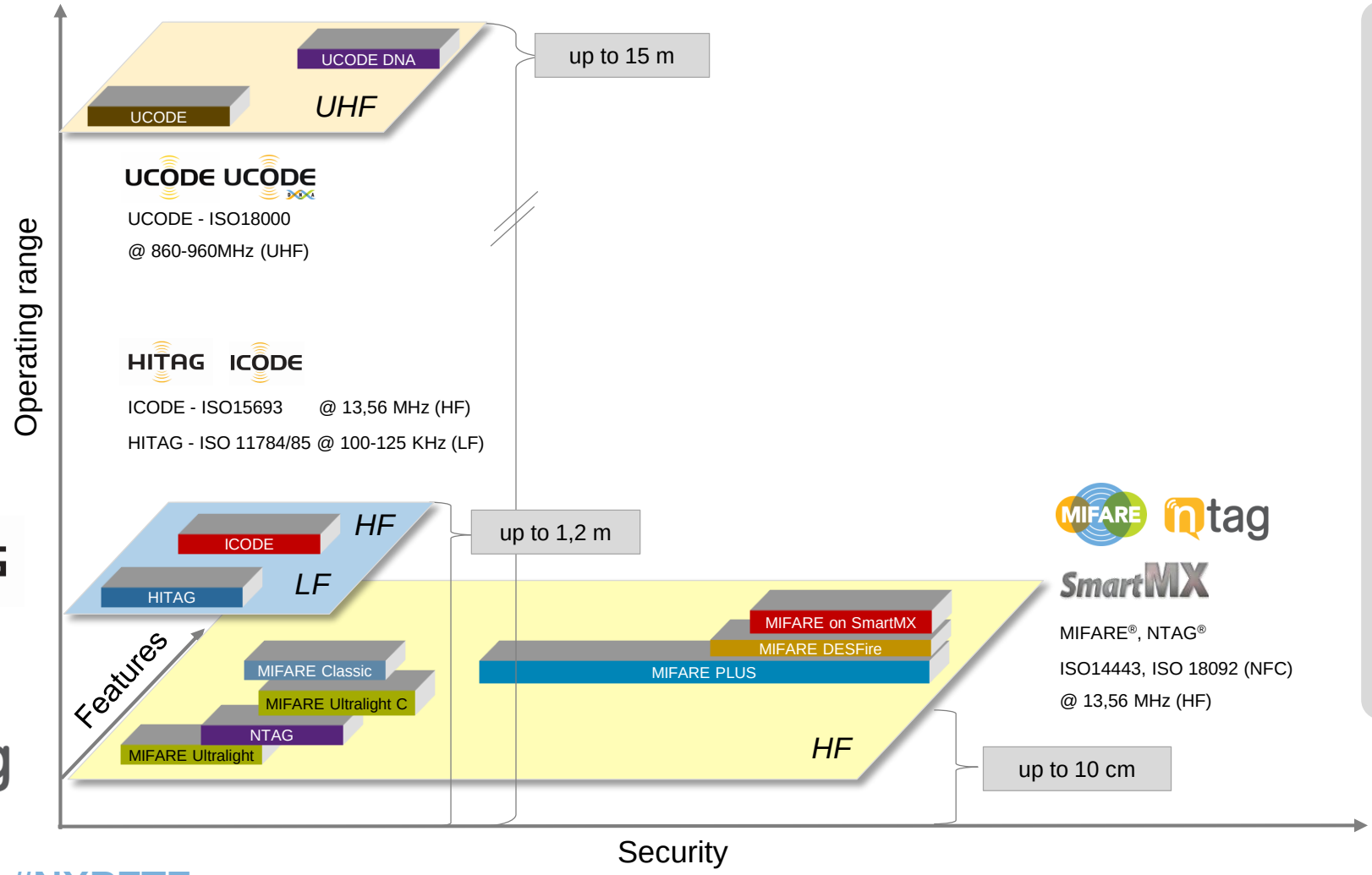
AGENDA

- MIFARE Plus Product positioning within portfolio
- Target markets & applications
- Why MIFARE Plus?
- Value proposition
- MIFARE Plus EV1

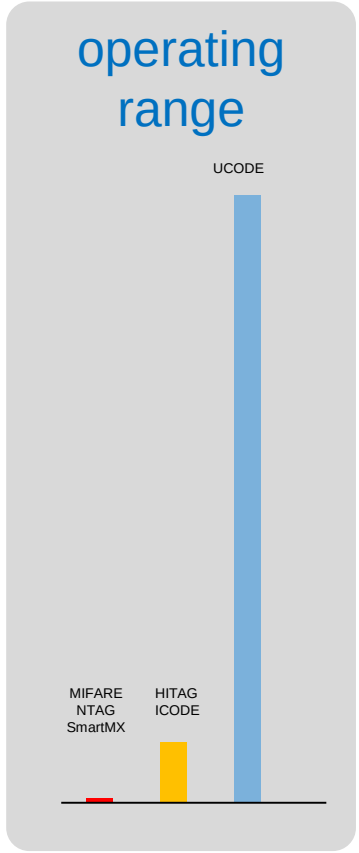
PRODUCT POSITIONING

NXP Contactless Tag IC Families

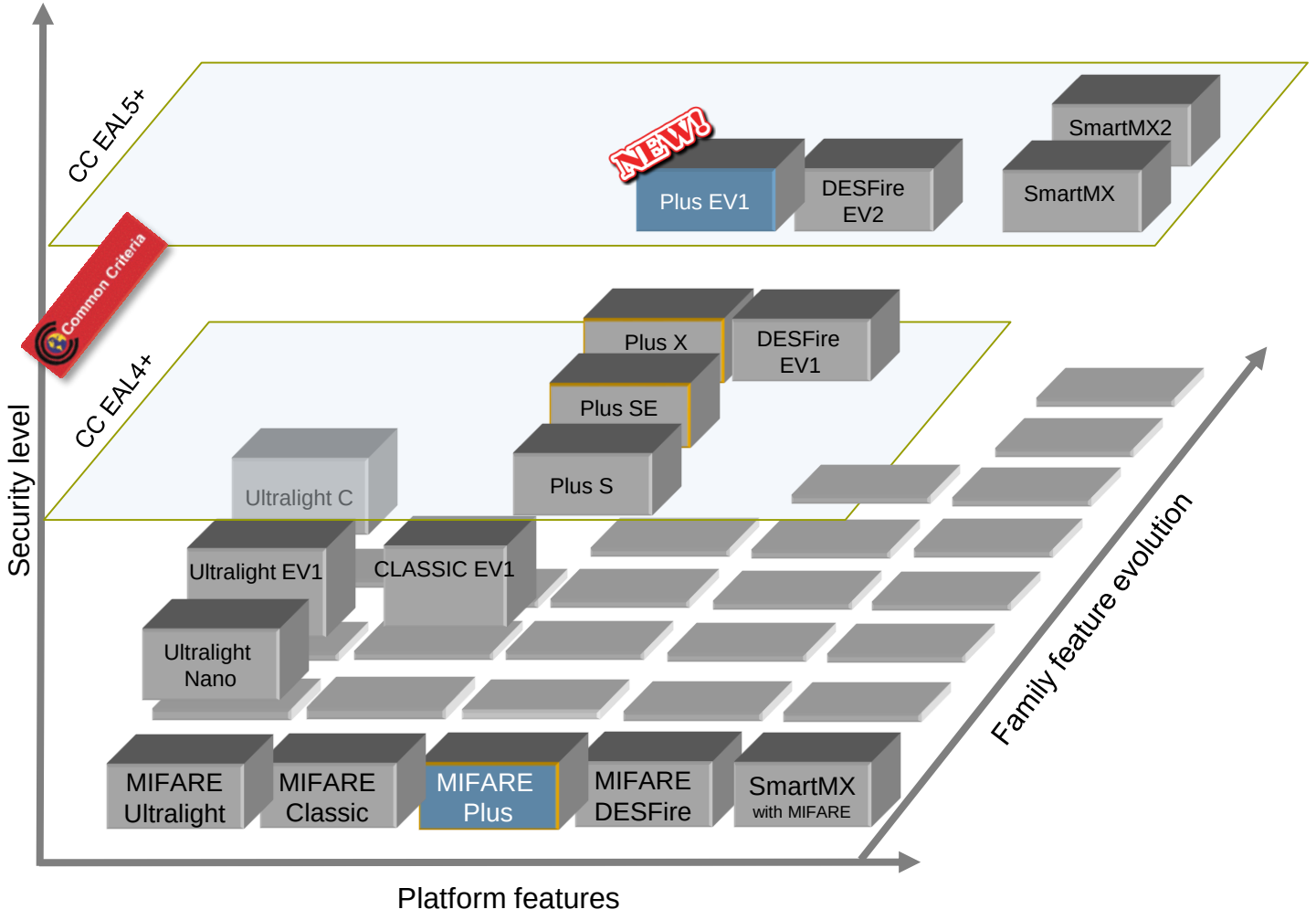
Relative positioning operating range vs. features and data security



MIFARE®, NTAG®
ISO14443, ISO 18092 (NFC)
@ 13,56 MHz (HF)



MIFARE Plus EV1 Positioning



TARGET MARKETS & APPLICATIONS

Target Applications

- 40 different Applications globally are based on MIFARE Classic and MIFARE Plus

WHY MIFARE PLUS?

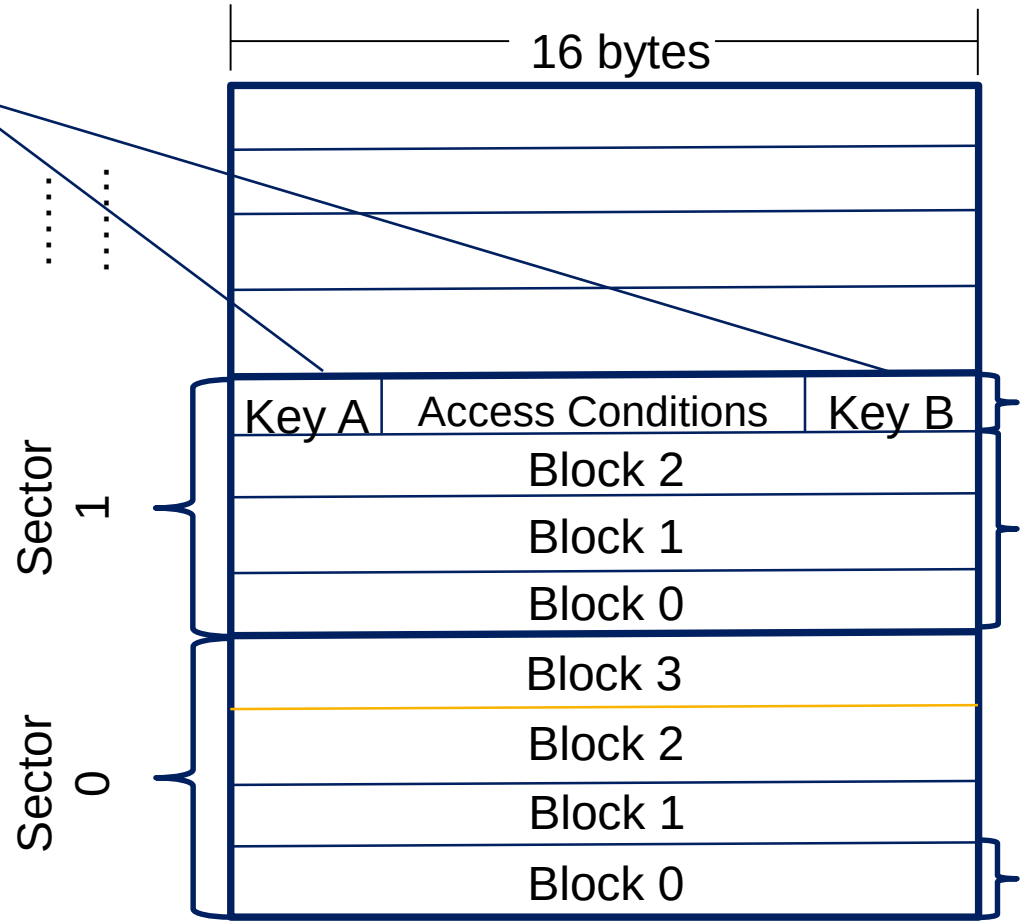
MIFARE Classic® Product Family

- Most used smartcard IC worldwide
- Enabling public transport in > 300 cities
- Powering more than 40 applications worldwide

- Key Features of MIFARE Classic EV1
  - 1KB or 4KB memory
  - 4B NUID or 7B UID
  - 48-bit Crypto1 security
  - Linear memory structure

Memory Structure – Linear Memory

MIFARE Classic
48-bit Crypto1



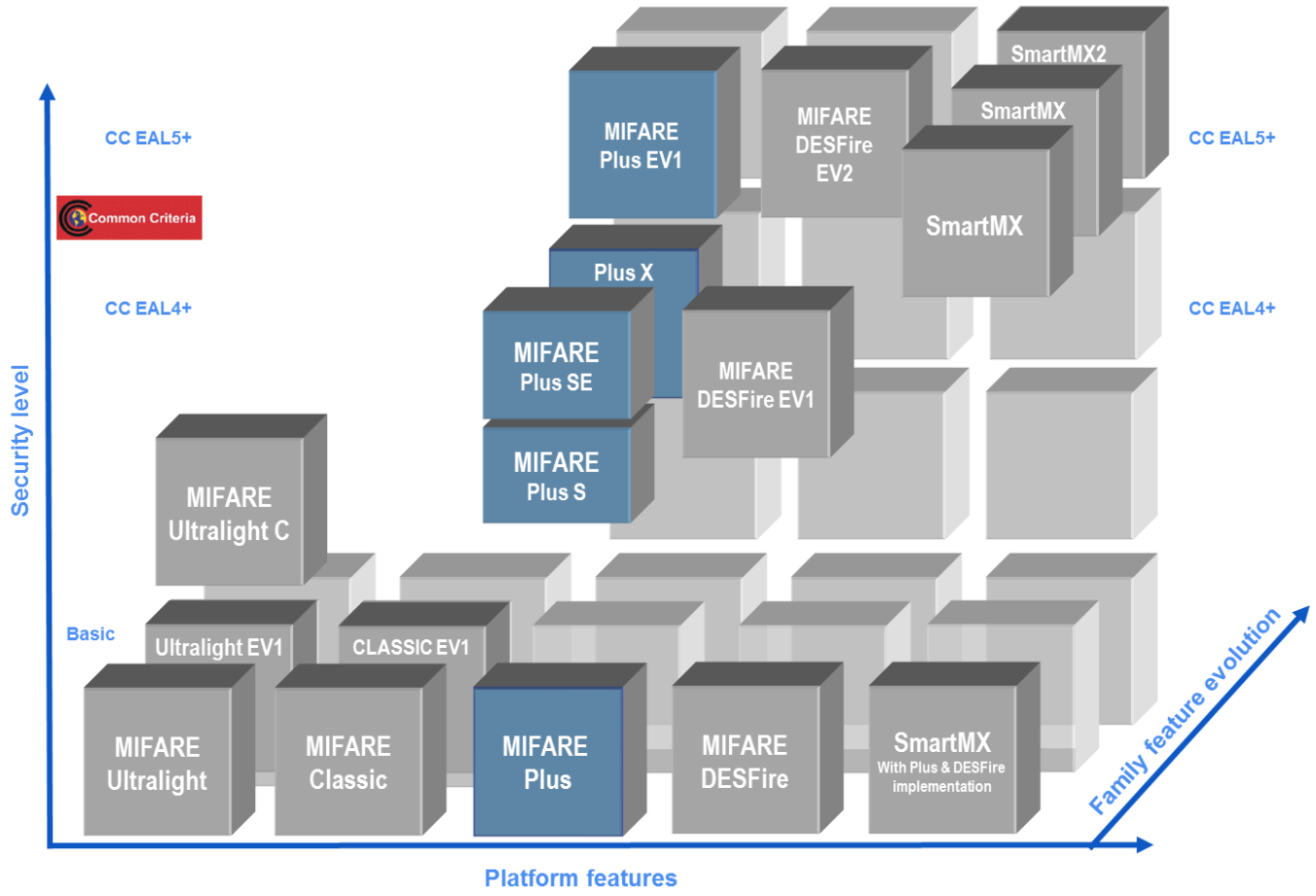
Sector Trailer

- for customer data
- for values (enables value operations)

Sector 0, Block 0 contains (N)UID & production specific data

Reasons to Migrate to a New Platform

- after more than 20 years security requirements increased
- NFC support needed
- But still leveraging from existing infrastructure installed base



VALUE PROPOSITION

MIFARE Plus – Scalable – Flexible – Future Proof

Latest features on highest security level

Secure

Securing the value of millions of end customers with benchmark AES security

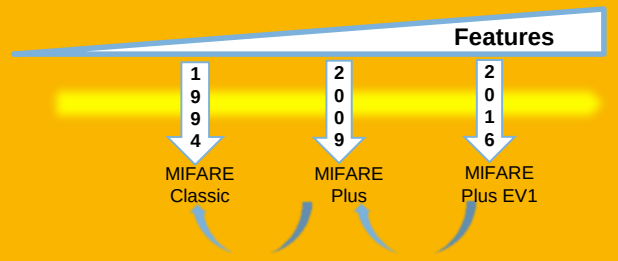
- **128-bit AES based on global standards**
- **CC certified product family**
- **Transaction MAC**

Field Proven

>15 million transactions/day

Dozens of cities including mega cities like Moscow, Sao Paulo,… on MIFARE Plus®

Sustainable



MIFARE Plus

>130Mpcs shipped

>150% annual growth

in average for the last 4 years

Public Transport

Access Management

Loyalty Cards

> 40 others

Fixed Memory Structure

Crypto1 and **128-bit AES** ISO 14443 compliant

Security **upgrade solution** for MIFARE Classic

Also available as **implementation on SmartMX** for DIF cards and eSE

Licensed to **>5 companies**

An **EV**olving platform staying ahead in **performance, security, privacy** and **multi-application support**

MIFARE Plus Product Family

Continuous evolution and interoperability

1994
MIFARE Classic

2009
MIFARE Plus

06/2015
MIFARE Plus SE

06/2016
MIFARE Plus EV1

Increased feature set on highest security level

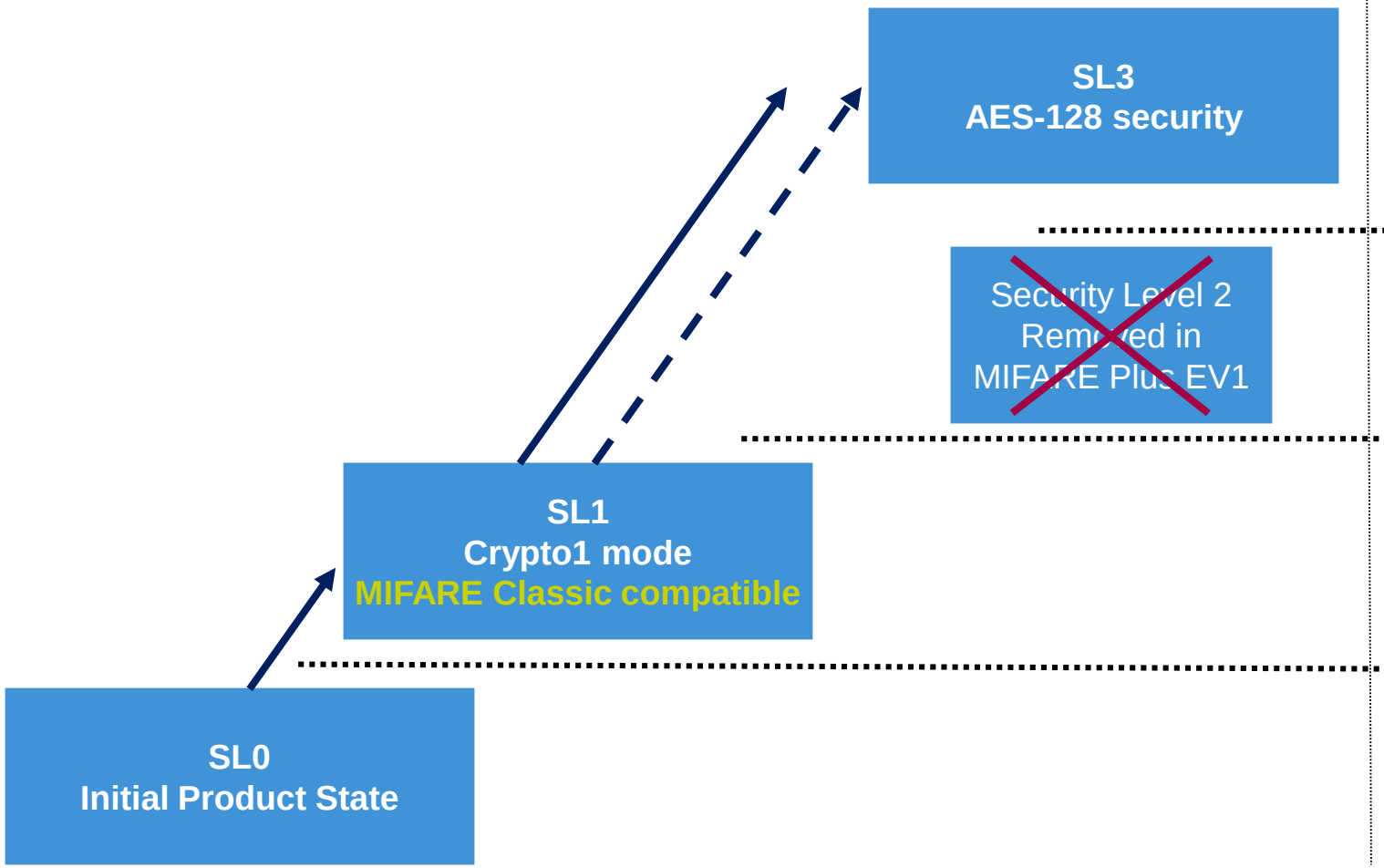
Cost-effective system environment upgrades

features:

- sector-wise security level upgrades
- e2e secure channel communication even for legacy Crypto1 sectors
- ISO 7816-4 wrapping
- TMAC for clearing house validation
- Improved interface for advanced tapping experience

MIFARE PLUS EV1

MIFARE Plus EV1 – Simplified Security Level Concept



Key features per security level

- AES-128 for authentication, integrity
- Multi sector authentication
- Multi-Block Read & Write
- Transaction MAC
- Optional Random ID
- Anti-tearing for keys & sector trailers & data

- Functional backwards compatible with MIFARE Classic
- Optional AES-128 authentication
- Optional AES-128 secure channel
- Sector Level Security Level Switching
- Transaction MAC

Personalization level, including:

- Program AES level switching keys (mandatory)
- Program Crypto1 & AES keys per sector (recommended)

MIFARE Plus® EV1 Features

Backwards Compatible

Functional backwards compatible to MIFARE Classic – Seamless upgrade path to AES security
Functional backwards compatible to MIFARE Plus EV0 – Easy replacement

Future-proof Investment

End2End Secure Channel – Fully secure over-the air card management even for Crypto1 sectors
SL1SL3 Mix Mode – Upgrade relevant applications only, save on system upgrade cost
Transaction MAC – Fraudulent transaction claim protection
Fully ISO compliant Proximity Check – Relay attack protection
Virtual Card Architecture – Privacy protection

Performance

Optimum transaction speed vs security – Fast & reliable transactions
New front-end – Achieving optimal performance
High-cap versions available – Suitable for small form factor

MIFARE PLUS EV1 – Key Features

Allows for selective system security upgrades and enables new, over-the-air value stream possibilities

Sector-wise security upgrade from Crypto1 to 128-bit AES

Upgrade security relevant applications only instead of whole system – save on overall system upgrade cost

Card top-up via mobile phone / no need for additional infrastructure

Secure end2end channel communication even for legacy crypto

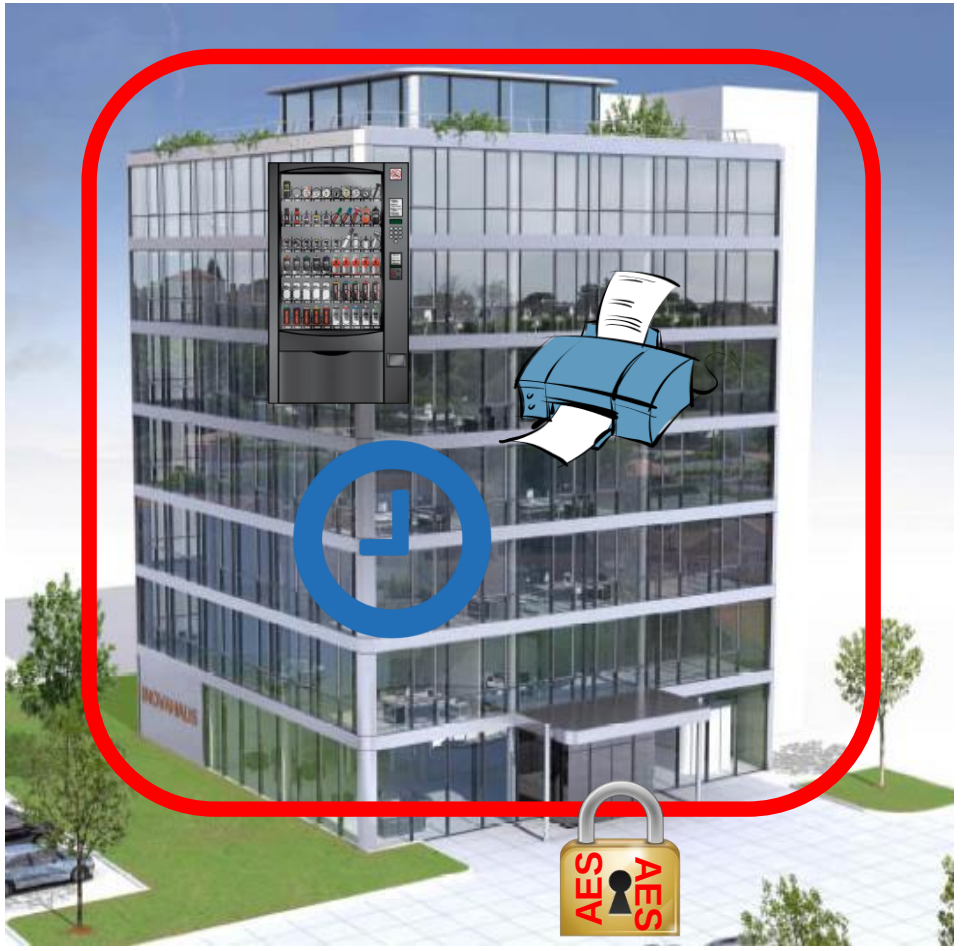
Enable combined service offerings for end-users

Transaction MAC ensuring that no fraudulent claims can be made by merchants

Nutshell Security Concept for Physical Access Control

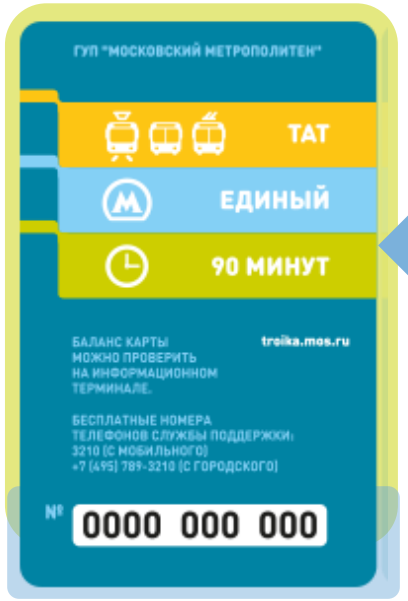
Sector-wise security level switching

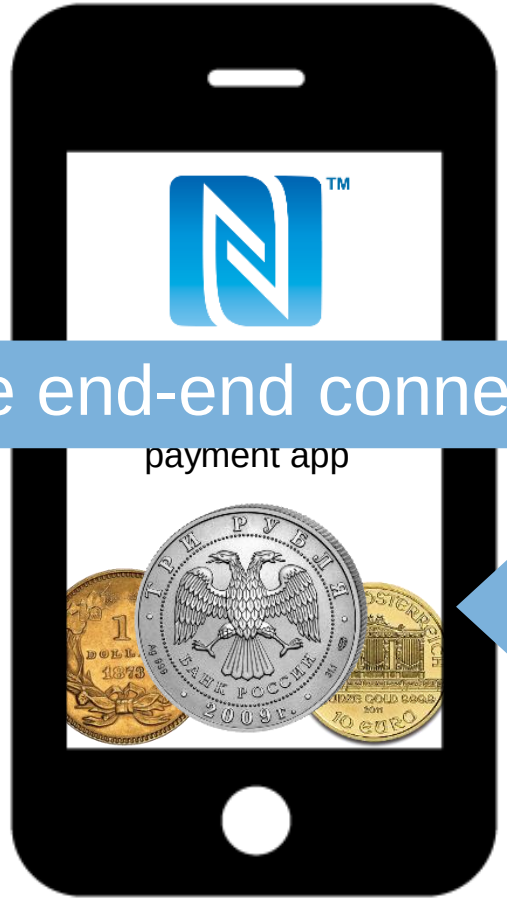
- Different security layers possible
- Reduce system upgrade effort and complexity
- Reduce system upgrade cost



Secure Over-the-air Services – eg. Top-up Services
Optional AES secure channel in SL1

Card personalized to SL1





Secure end-end connection

- 128-bit AES secure
- full data encryption
- full integrity protection
- write values to any card sector

AES key for secure channel communication

Secure connection to service provider

- choose and pay for eg. a 1 day ticket
- choose and pay the top-up for your card for eg. for vending machines
- …….

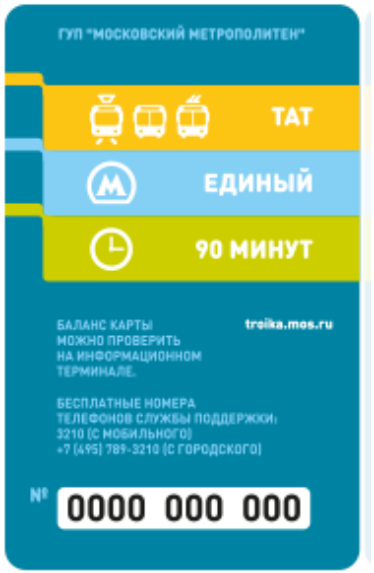
Secure Over-the-air Services – eg. Top-up Services

Business Need	Advantages Value Chain	Advantages System Operators
Issue Premium Cards	• Sell high value prints • Charge min. premium for add. personalization effort	• Charge premium for premium market segment • Tailored service offering for each customer segment
Upgrade security relevant applications	• Upsell to existing customers • Address additional customer groups	• Implement additional services for end customers • Minimize implementation cost
Remote card management	• Personalize cards in the field • Upgrade cards in the field • Easily load credentials	• Simple maintenance • Simple deployment of new, secure applications

Enable Offline Transactions with Secure Verification

Transaction MAC

- Secure verification of transaction validity
- Adding offline capabilities
- Establish trust in multi-service provider systems



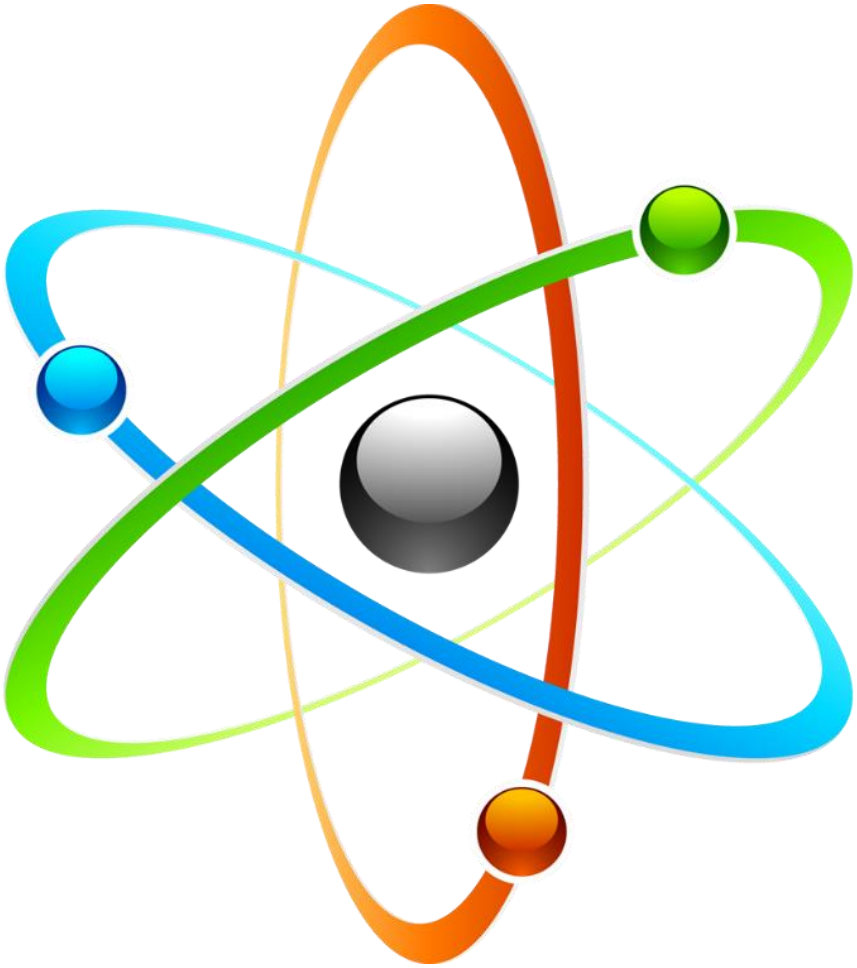
Valid offline transaction

TMAC with transaction data stored in reader

MIFARE Plus EV1 Eco-system Roadmap

- MIFARE Plus Applet – Q4 2016
  For easy integration into mobile environments

- MIFARE4Mobile integration – end 2016
  Standard for using MIFARE Plus EV1 in SEs



SECURE CONNECTIONS
FOR A SMARTER WORLD

ATTRIBUTION STATEMENT